Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования
«Санкт-Петербургский государственный университет промышленных технологий и дизайна»
ВЫСШАЯ ШКОЛА ТЕХНОЛОГИИ И ЭНЕРГЕТИКИ

УТВЕРЖДАЮ
Директор ВШТЭ

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 7d15b88066d31dcb1847af0d7d99b718672f8b21
Владелец: Лукашин Павел Владимирович
Действителен: с 11.02.2020 по 31.12.2022

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.06 — **Информационная безопасность**
(индекс дисциплины) — *(Наименование дисциплины)*

Кафедра: **16** Прикладной математики и информатики
Код — *(Наименование кафедры)*

Направление подготовки: 01.03.02 Прикладная математика и информатика

Профиль подготовки: Прикладная математика и информатика

Уровень образования: бакалавриат

План учебного процесса

Составляющие учебного процесса		Очное обучение	Очно-заочное обучение	Заочное обучение
Контактная работа обучающихся с преподавателем по видам учебных занятий и самостоятельная работа обучающихся (часы)	Всего	**180**		
	Аудиторные занятия	**56**		
	Лекции	28		
	Лабораторные занятия			
	Практические занятия	28		
	Самостоятельная работа	**124**		
	Промежуточная аттестация			
Формы контроля по семестрам (номер семестра)	Зачет	8		
Общая трудоемкость дисциплины (зачетные единицы)		**5**		

Форма обучения:	Распределение зачетных единиц трудоемкости по семестрам									
	1	2	3	4	5	6	7	8	9	10
Очная								**5**		
Очно-заочная										
Заочная										

Санкт-Петербург
2020

Рабочая программа дисциплины составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 010302 Прикладная математика и информатика

На основании учебных планов № b010302-3_20

Кафедра-разработчик: Прикладной математики и информатики

Заведующий кафедрой: Яковлев В.П.

СОГЛАСОВАНИЕ:

Выпускающая кафедра: Прикладной математики и информатики

Заведующий кафедрой: Яковлев В.П.

Методический отдел: Смирнова В.Г.

1. ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1. Место преподаваемой дисциплины в структуре образовательной программы

Блок 1:	Базовая		Обязательная		Дополнительно является факультативом
	Вариативная	X	По выбору		

1.2. Цель дисциплины

ознакомление с организационными, техническими, и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области, изучение методов защиты информации.

1.3. Задачи дисциплины

- Задачей изучения дисциплины является усвоение студентами основ информационной безопасности — источников, рисков и форм атак на информацию . Учащиеся должны уметь определять вредоносные программы и компьютерные вирусы. В процессе изучения предмета они приобретают знания в области правовых основ, политики и стандартов информационной безопасности. Происходит их знакомство с криптографическими моделями, алгоритмами шифрования, а с также антивирусной защитой и требованиями к системам информационной защиты ИС.

1.4. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Формулировка компетенции	Этап формирования
ПК-2	способностью понимать, совершенствовать и применять современный математический аппарат	2

Планируемые результаты обучения

Знать:

1) базовые теоретические положения в области информационной безопасности;
2) методы и средства решения задач профессиональной деятельности с учетом основных требований информационной безопасности.

Уметь:

1) использовать базовые теоретические положения дисциплины «Информационная безопасность» в профессиональной деятельности;
2) решать задачи профессиональной деятельности с учетом основных требований информационной безопасности.

Владеть:

1) навыками использования информационно-коммуникационных технологий с учетом основных требований информационной безопасности.
2) навыками выбора методов решения задач профессиональной деятельности на основе теоретических знаний в области информационной безопасности.

1.5. Дисциплины (практики) образовательной программы, в которых было начато формирование компетенций, указанных в п.1.4:

- Операционные системы (ПК-2);
- Теория игр и исследование операций (ПК-2);
- Теория вероятностей и математическая статистика (ПК-2);
- Дискретная математика (ПК-2).

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
Учебный модуль 1. Введение в информационную безопасность.			
Тема 1. Основные понятия и определения.	25		
Модели информационной безопасности. Виды защищаемой информации. Обзор источников, рисков и форм атак на информацию в ИС, вредоносных программ и компьютерных вирусов. Проблемы защиты информации в ИС.			
Тема 2. Правовые основы информационной безопасности.	24		
Основные нормативно-правовые акты в области информационной безопасности. Защита конфиденциальной информации. Политика информационной безопасности. Содержание основных документов предприятия по обеспечению защиты компьютерной информации в ИС			
Текущий контроль 1: Устный опрос № 1	1		
Учебный модуль 2. Шифрование данных.			
Тема 3. Основы криптографии.	25		
Криптографические модели. Симметричные и ассиметричные криптосистемы для защиты компьютерной информации в ИС. Цифровые (электронные) подписи. Инфраструктура открытых ключей. Криптографические протоколы.			
Тема 4. Стандартные алгоритмы шифрования.	25		
Безопасность и быстродействие криптосистем. Зашифровывание и расшифровывание. Криптостойкость шифра. Абсолютно стойкие системы. Достаточно стойкие системы. Симметричное и асимметричное шифрование. Схемы их реализации. Управление ключами.			
Тема 5. Разработка программного обеспечения по шифрованию данных в среде объектно-ориентированного программирования.	24		
Шифр Цезаря как частный случай шифра подстановки. Шифр Атбаш. Шифр Виженера. Одноразовый блокнот. Шифр перестановки. Шифр маршрутной перестановки. Шифр двойной перестановки.			
Текущий контроль 2: Устный опрос № 2	1		
Учебный модуль 3. Внедрение и сопровождение информационных систем			
Тема 6. Базовые понятия защиты информации в компьютерных сетях.	25		
Методы идентификации и проверки подлинности пользователей компьютерных систем. Основные этапы допуска к ресурсам компьютерной системы. Многоуровневая защита корпоративных сетей. Защита компьютерных систем от удаленных атак через сеть Internet. Настройка и использование файрволов.			
Тема 7. Антивирусная защита.	29,75		
Классификация компьютерных вирусов. Основные этапы жизненного цикла вирусов. Объекты внедрения, режимы функционирования и специальные функции вирусов. Разработка и основные принципы использования антивирусного программного обеспечения.			
Текущий контроль 3: Устный опрос № 3	1		
Промежуточная аттестация по дисциплине - Зачет	**0,25**		
ВСЕГО:	**180**		

3. ТЕМАТИЧЕСКИЙ ПЛАН

3.1. Лекции

Номера изучаемых тем	Очное обучение		Очно-заочное обучение		Заочное обучение	
	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
1	8	4				
2	8	4				
3	8	4				
4	8	4				

Номера изучаемых тем	Очное обучение		Очно-заочное обучение		Заочное обучение	
	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
5	8	4				
6	8	4				
7	8	4				
	ВСЕГО:	**28**				

3.2. Практические занятия

Номера изучаемых тем	Наименование и форма занятий	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
1	Закрепление теоретических знаний по существующим моделям информационной безопасности	8	2				
1	Анализ рисков информационной безопасности	8	2				
2	Закрепление теоретических знаний в области правового обеспечения информационной безопасности	8	2				
2	Закрепление теоретических знаний по вопросам государственного лицензирования деятельности в области защиты информации	8	2				
3	Закрепление теоретических знаний по вопросам сертификации средств криптографической защиты информации	8	2				
3	Изучение механизма контроля целостности данных (работа с электронно-цифровой подписью)	8	2				
4	Изучение симметричных криптосистем	8	2				
4	Изучение ассимметричных криптосистем	8	2				
5	Программирование арифметических криптографических алгоритмов	8	2				
5	Программирование алгебраических криптографических алгоритмов	8	2				
6	Построение концепции информационной безопасности предприятия	8	2				
6	Изучение процедуры аутентификации пользователя на основе пароля	8	2				
7	Изучение пакетов антивирусных программ	8	2				
7	Изучение алгоритмов	8	2				

Номера изучаемых тем	Наименование и форма занятий	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
	предупреждения и обнаружения вирусных угроз						
	ВСЕГО:		**28**				

3.3. Лабораторные занятия

Не предусмотрены

4. КУРСОВОЕ ПРОЕКТИРОВАНИЕ

Не предусмотрено

5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ ОБУЧАЮЩЕГОСЯ

Номера учебных модулей, по которым проводится контроль	Форма контроля знаний	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Кол-во	Номер семестра	Кол-во	Номер семестра	Кол-во
1-3	Устный опрос	8	3				

6. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ

Виды самостоятельной работы обучающегося	Очное обучение		Очно-заочное обучение		Заочное обучение	
	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
Усвоение теоретического материала	8	50				
Подготовка к практическим занятиям	8	68				
Подготовка к зачету	8	6				
ВСЕГО:		**124**				

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

7.1. Характеристика видов и используемых инновационных форм учебных занятий

Не предусмотрены

7.2. Система оценивания успеваемости и достижений обучающихся для промежуточной аттестации

традиционная [X] балльно-рейтинговая [ ]

8. ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Учебная литература

а) основная учебная литература

1. Башлы П. Н., Бабаш А. В., Баранова Е. К. [Электронный ресурс]: учебное пособие/ Информационная безопасность и защита информации. — Москва: Евразийский открытый институт, 2012. — Режим доступа: http://www.iprbookshop.ru/10677.html;

2. Прохорова О. В. [Электронный ресурс]: учебное пособие/ Информационная безопасность и защита информации. — Самара: Самарский государственный архитектурно- строительный университет, ЭБС АСВ, 2014. — Режим доступа: http://www.iprbookshop.ru/43183.html;

б) дополнительная учебная литература

3. Горев А. И., Симаков А. А. [Электронный ресурс]: учебное пособие/ Обработка и защита информации в компьютерных системах. — Омск: Омская академия МВД России, 2016. — Режим доступа: http://www.iprbooksh op.ru/72856.html;

4. Никифоров С. Н. [Электронный ресурс]: учебное пособие/ Защита информации. — Санкт-Петербург: Санкт- Петербургский государственный архитектурно- строительный университет, ЭБС АСВ, 2015. — Режим доступа: http://www.iprbookshop.ru/74365.html.

8.2. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

1. Никифоров С. Н. [Электронный ресурс]: учебное пособие/ Защита информации. — Санкт-Петербург: Санкт- Петербургский государственный архитектурно- строительный университет, ЭБС АСВ, 2015. — Режим доступа: http://www.iprbookshop.ru/74365.html.

8.3. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины

1. Электронно-библиотечная система IPRbooks [Электронный ресурс]. URL: http://www.iprbookshop.ru/
2. Электронная библиотека ВШТЭ СПБ ГУПТД [Электронный ресурс]. URL: http://nizrp.narod.ru
3. Информационная система «Единое окно доступа к образовательным ресурсам. Раздел. Информатика и информационные технологии» [Электронный ресурс]. URL: http://window.edu.ru/

8.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

1. Microsoft Windows 8.1;
2. Microsoft Office Professional 2013.

8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

1. Лекционная аудитория с мультимедийным учебным комплексом
2. Компьютерный класс с мультимедийным комплексом и выходом в Интернет

8.6. Иные сведения и (или) материалы

1. Демонстрационные материалы по темам лекций и практических занятий.
2. Раздаточные материалы по темам лекций и практических занятий.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Виды учебных занятий и самостоятельная работа обучающихся	Организация деятельности обучающегося
Лекции	Проработка рабочей программы, с обращением особого внимания целям и задачам структуре и содержанию дисциплины. Конспект лекций: кратко, схематично, последовательно фиксировать основные положения, выводы и формулировки; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий: осуществлять с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Работа с теоретическим материалом: найти ответ на вопросы в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации или на практическом занятии.
Практические занятия	Подготовка к практическим занятиям предполагает следующие виды работ: • работа с конспектом лекций; • подготовка ответов к контрольным вопросам; • просмотр рекомендуемой литературы, работа с текстом; • решение задач по алгоритму.
Самостоятельная работа	Данный вид работы предполагает расширение и закрепление знаний, умений и навыков, усвоенных на аудиторных занятиях путем самостоятельной проработки учебно-методических материалов по дисциплине и другим

Виды учебных занятий и самостоятельная работа обучающихся	Организация деятельности обучающегося
	источникам информации; подготовку к устным опросам и экзамену. Самостоятельная работа выполняется индивидуально, а также может проводиться под руководством (при участии) преподавателя. При подготовке к зачету необходимо ознакомиться с перечнем вопросов, проработать конспекты лекций и практических занятий, рекомендуемую литературу, получить консультацию у преподавателя.

10. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

10.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

10.1.1. Показатели оценивания компетенций на этапах их формирования

Код компетенции (этап освоения)	Показатели оценивания компетенций	Наименование оценочного средства	Представление оценочного средства в фонде
ПК-2 (2)	1. Излагает базовые теоретические положения по дисциплине, имеет представление: • о методах и средствах решения задач профессиональной деятельности с учетом основных требований информационной безопасности. 2. Демонстрирует умение: • решать задачи профессиональной деятельности с учетом основных требований информационной безопасности. 3. Показывает навыки: • использования информационно-коммуникационных технологий с учетом основных требований информационной безопасности. • выбора методов решения задач профессиональной деятельности на основе теоретических знаний в области информационной безопасности.	1. Устное собеседование 2. Практическое задание	1. Перечень вопросов к зачету (24 вопроса). 2. Практические задания (12 заданий).

10.1.2. Описание шкал и критериев оценивания сформированности компетенций. Критерии оценивания сформированности компетенций

Критерии оценивания сформированности компетенций

Оценка по традиционной шкале	Критерии оценивания сформированности компетенций
Зачтено	Обучающийся твердо знает материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопросы, способен правильно применить основные методы и инструменты при решении практических задач, владеет необходимыми навыками и приемами их выполнения.
Не зачтено	Обучающийся не может изложить значительной части программного

	материала, допускает существенные ошибки, допускает неточности в формулировках и доказательствах, нарушения в последовательности изложения программного материала; неуверенно, с большими затруднениями выполняет практические задания.

10.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

10.2.1. Перечень вопросов к зачету, разработанный в соответствии с установленными этапами формирования компетенций

№ п/п	Формулировка вопросов	№ темы
1	Прогресс информационных технологий и необходимость обеспечения информационной безопасности.	1
2	Основные понятия информационной безопасности.	1
3	Система защиты информации и ее структура	2
4	Информация как товар и объект безопасности.	2
5	Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.	2
6	Персональные данные и их защита.	3
7	Информационные угрозы, их виды и причины возникновения.	3
8	Способы воздействия информационных угроз на объекты.	3
9	Внешние и внутренние субъекты информационных угроз.	3
10	Вредоносные программы, их виды.	3
11	История компьютерных вирусов и современность.	3
12	Политика безопасности и ее принципы.	3
13	Фрагментарный и системный подход к защите информации	4
14	Методы и средства защиты информации.	4
15	Организационное обеспечение информационной безопасности	4
16	Организация конфиденциального делопроизводства.	4
17	Комплекс организационно-технических мероприятий по обеспечению защиты информации.	5
18	Инженерно-техническое обеспечение компьютерной безопасности.	6
19	Защита информации в Интернете	6
20	Защита от компьютерных вирусов.	7
21	Популярные антивирусные программы и их классификация.	7
22	Организация системы защиты информации экономических объектов.	7
23	Криптографические методы защиты информации.	7
24	Этапы построения системы защиты информации.	7

10.2.2 Вариант типовых заданий (задач), разработанных в соответствии с установленными этапами формирования компетенций

№ п/п	Условия типовых задач	Ответ

1	Разработать в современной среде программирования приложение, реализующее шифр Цезаря	Пример выполнения задания на языке С++
		
		#include <stdio.h>
		#include <conio.h>
		#include <string.h>
		int main()
		{
		int i=0, n=0, k;
		int d;
		char alf[] = "abcedfghijklmnopqrstuvwxyz0123456789#!@$%^&*-+=";//словарь
		char buf[10];
		char decod[10];

		printf("\n Caesar encryption program \n");
		
		/*Процедура шифрования */
		printf("\n *** Encryption *** ");
		printf("\n Enter a word or number:");
		scanf("%s",&buf);//ввод слова или числа
		printf("\n Enter numeric key (step from 1 to10): ");
		scanf("%i",&k);//вводим ключ
		for (n=0; n < 10; n++)
		{
		for (i = 0; i < 47; i++)
		{
		if (buf[n] == alf[i])
		{
		if (i >= 47)
		buf[n] = alf[i-47];
		else
		buf[n] = alf[i+k];
		break;
		}
		}
		}
		printf("\nVash shefr= %s\n", buf);//выводим полученный шифр
		
		/*Процедура дешифрования*/
		printf("\n Deciphering \n");
		printf("\n Enter your code : ");
		scanf("%s",&decod); //вводим шифр
		printf("\n Enter numeric key (step from 1 to10): ");
		scanf("%i",&d); //вводим ключ
		for (n=0; n < 10; n++)
		{
		for (i = 0; i < 47; i++)
		{
		if (decod[n] == alf[i])
		{
		if (i >= 47)
		decod[n] = alf[i-47];
		else
		decod[n] = alf[i-d];//
		break;// }
		}
		}
		printf("\nShefr= ");
		puts (decod);// выводим код
		getch();//
		return 0;
		}

2	Разработать в современной среде программирования приложение, реализующее шифрование методом магического квадрата	Пример выполнения задания на языке Pascal ABC
		
		begin
		writeln('Введите слово');
		readln(s);
		while n * n < length(s) do inc(n);
		while length(s) < n * n do s := s + ' ';
		writeln('Магический Квадрат');
		for i := 1 to n do
		begin
		for j := 1 to n do
		begin
		a[i, j] := 1 + ((i - j + (n - 1) div 2) mod n) * n + ((i + j + (n + 1) div 2) mod n);
		if a[i, j] < 0 then a[i, j] := n * n + a[i, j];

		b[i, j] := s[a[i, j]];
		write(a[i, j]:4);
		end;
		writeln;
		end;
		writeln('Зашифрованный текст:');
		for i := 1 to n do
		for j := 1 to n do
		write(b[i, j]);
		writeln;
		writeln('Расшифрованный текст:');
		for i := 1 to n do
		for j := 1 to n do c[a[i, j]] := b[i, j];
		for i := 1 to n * n do write(c[i]);
		end.

10.3. Методические материалы, определяющие процедуры оценивания знаний, умений, владений (навыков и (или) практического опыта деятельности), характеризующих этапы формирования компетенций

10.3.1. Условия допуска обучающегося к сдаче зачета и порядок ликвидации академической задолженности

Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся

10.3.2. Форма проведения промежуточной аттестации по дисциплине

устная	X	письменная		компьютерное тестирование		иная*	

10.3.3. Особенности проведения зачета

- Возможность пользоваться справочным материалом;
- Время на подготовку ответа по билету 15 минут;
- Зачет проводится в компьютерном классе.